

# THE SPLITTING SUBSPACE CONJECTURE

ERIC CHEN AND DENNIS TSENG

**ABSTRACT.** We answer a question by Niederreiter concerning the enumeration of a class of subspaces of finite dimensional vector spaces over finite fields by proving a conjecture by Ghorpade and Ram.

## 1. INTRODUCTION

We positively resolve the Splitting Subspace Conjecture, stemming from a question posed by Niederreiter (1995) [4, p. 11] and stated by Ghorpade and Ram [3]. The conjecture was inspired by earlier work from Zeng, Han and He [5] and Ghorpade, Hasan and Kumari [2]. We first define the notion of a  $\sigma$ -splitting subspace.

**Definition.** In the vector space  $\mathbb{F}_{q^{mn}}$  over the finite field  $\mathbb{F}_q$ , given a  $\sigma \in \mathbb{F}_{q^{mn}}$  such that  $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\sigma)$ , a ( $m$ -dimensional) subspace  $W$  of  $\mathbb{F}_{q^{mn}}$  is a  $\sigma$ -splitting subspace if

$$W \oplus \sigma W \oplus \cdots \oplus \sigma^{n-1} W = \mathbb{F}_{q^{mn}}.$$

For example,  $\{1, \sigma^m, \sigma^{2m}, \dots, \sigma^{(n-1)m}\}$  spans a  $\sigma$ -splitting subspace. If  $n = 1$ , then  $\mathbb{F}_{q^m}$  is the only  $\sigma$ -splitting subspace; if  $m = 1$ , then each 1-dimensional subspace of  $\mathbb{F}_{q^n}$  is  $\sigma$ -splitting.

**Conjecture 1** (Ghorpade-Ram). The number of  $\sigma$ -splitting subspaces is

$$\frac{q^{mn} - 1}{q^m - 1} q^{m(m-1)(n-1)}.$$

This follows as Corollary 3.4 from our main result, Theorem 3.3. The next two sections are devoted to proving this theorem. We first construct a recursion that gives the cardinality of more general classes of subspaces, including the  $\sigma$ -splitting subspaces, and then solve this recurrence to obtain the result. Finally, we discuss some special cases of our more general result.

## 2. RECURSION

For the remainder of this article, unless otherwise noted, consider more generally the vector space  $\mathbb{F}_{q^N} (= \mathbb{F}_q^N)$  over the finite field  $\mathbb{F}_q$ , given a  $\sigma \in \mathbb{F}_{q^N}$  such that  $\mathbb{F}_{q^N} = \mathbb{F}_q(\sigma)$ .

We begin by isolating the key property of the linear transformation  $v \mapsto \sigma v$ .

**Proposition 2.1.** *The linear endomorphisms of  $\mathbb{F}_{q^N}$  that preserve no subspaces other than  $\{0\}$  and all of  $\mathbb{F}_{q^N}$  are exactly those which act as multiplication by a primitive element  $\sigma$  that generates the extension  $\mathbb{F}_q(\sigma) = \mathbb{F}_{q^N}$ .*

---

Date: August 3, 2012.

*Proof.* Operators defined as multiplication by a primitive element  $\sigma$  generating the extension  $\mathbb{F}_q(\sigma) = \mathbb{F}_{q^N}$  cannot preserve any subspaces except  $\{0\}$  and  $\mathbb{F}_{q^N}$ , for if  $W$  is such a subspace with nonzero  $w \in W$ , then  $w \sum_{i=0}^{N-1} a_i \sigma^i \in W$ ,  $a_i \in \mathbb{F}_q$ , so  $W = \mathbb{F}_{q^N}$ . Conversely, note that any linear operator  $T$  together with the vector space  $\mathbb{F}_q^N$  can be viewed as a finitely generated  $\mathbb{F}_q[x]$  module  $M$ , where  $x$  acts as  $T$ . Since  $\mathbb{F}_q[x]$  is a principal ideal domain, we can use the primary decomposition of  $M$  to find  $M \cong \bigoplus_{i=1}^k \mathbb{F}_q[x]/(p_i(x)^{r_i})$ , where  $p_i$  is a polynomial for each  $i$  and  $r_i$  is a positive integer.

If  $T$  preserves no proper subspaces of  $\mathbb{F}_{q^N}$ , then  $k = 1$ . Also,  $r_1 = 1$  unless  $p_1(T)M$  is a proper submodule of  $M$ . Therefore, we have  $M$  is equal to  $\mathbb{F}_q[x]/(p_1(x))$ , where  $p_1$  is an irreducible polynomial. This is exactly what it means for  $x(=T)$  to act as the primitive element of the field extension  $\mathbb{F}_q(\sigma) = \mathbb{F}_{q^N} = \mathbb{F}_q^N$  with minimal polynomial  $p_1(x)$ .  $\square$

We next define notation to describe the sets to be counted by the general recursion.

**Definition.** Suppose that  $A_1, A_2, \dots, A_k$  are sets of subspaces of  $\mathbb{F}_{q^N}$ . Let  $[A_1, A_2, \dots, A_k]$  be the set of all  $k$ -tuples  $(W_1, W_2, \dots, W_k)$  such that

$$\begin{aligned} W_i &\in A_i \quad \text{for} \quad 1 \leq i \leq k, \\ W_i &\supseteq W_{i+1} + \sigma W_{i+1} \quad \text{for} \quad 1 \leq i \leq k-1. \end{aligned}$$

If  $A_i$  is the set of all subspaces of  $\mathbb{F}_{q^N}$  with dimension  $d_i$ , then  $A_i$  is denoted within the brackets as  $d_i$ . For example,  $[3, A_2]$  denotes all tuples  $(W_1, W_2)$  such that  $\dim(W_1) = 3$ ,  $W_2 \in A_2$  and  $W_1 \supseteq W_2 + \sigma W_2$ .

**Definition.** For nonnegative integers  $a, b$  with  $N > a > b$  or  $a = b = 0$

$$(a, b) := \{W \subseteq \mathbb{F}_{q^N} : \dim(W) = a \text{ and } \dim(W \cap \sigma^{-1}W) = b\}.$$

For example,  $(1, 0)$  is the set of all 1-dimensional subspaces and  $(2, 1)$  is the set of all 2-dimensional subspaces  $W$  such that  $\dim(W \cap \sigma^{-1}W) = 1$ .

**Definition.** Given sets  $[A_{1,1}, A_{1,2}], [A_{2,1}, A_{2,2}], \dots, [A_{r,1}, A_{r,2}]$  as defined above, let

$$\langle [A_{1,1}, A_{1,2}], [A_{2,1}, A_{2,2}], \dots, [A_{r,1}, A_{r,2}] \rangle$$

denote the set of  $2r$ -tuples of subspaces  $(W_{1,1}, W_{1,2}, W_{2,1}, W_{2,2}, \dots, W_{r,1}, W_{r,2})$  such that

$$\begin{aligned} (W_{i,1}, W_{i,2}) &\in [A_{i,1}, A_{i,2}] \quad \text{for} \quad 1 \leq i \leq r, \\ W_{i,2} &\supseteq W_{i+1,1} \quad \text{for} \quad 1 \leq i \leq r-1. \end{aligned}$$

For example,  $\langle [3, 2], [2, 1] \rangle$  is the set of all 4-tuples of subspaces  $(W_1, W_2, W_3, W_4)$  such that

$$\begin{aligned} \dim(W_1) &= 3, \quad \dim(W_2) = 2, \quad \dim(W_3) = 2, \quad \dim(W_4) = 1, \\ W_1 &\supseteq W_2 + \sigma W_2, \quad W_3 \supseteq W_4 + \sigma W_4, \\ W_2 &\supseteq W_3. \end{aligned}$$

We use the following proposition extensively in constructing the recursion.

**Proposition 2.2.** For nonnegative integers  $N > a > b$  or  $a = b = 0$

$$[a, b] = \bigcup_{i=b}^{\max(a-1, 0)} [(a, i), b]$$

$$= \bigcup_{j=0}^{\max(b-1,0)} [a, (b, j)].$$

*Proof.* Follows from Proposition 2.1 and the definitions of  $[\cdot, \cdot], (\cdot, \cdot)$ .  $\square$

We next define an ordering on the tuples labelling the sets of subspaces

$$[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})].$$

The recursion in Lemma 2.3 will give the cardinality of sets of subspaces so labelled in terms of the cardinality of sets labelled by tuples before it in the ordering. The base case is  $[(0, 0)]$ , containing one element.

**Definition.** First, define an ordering on the ordered pairs of the form  $(a, b)$  such that  $(a_1, b_1) \succ (a_2, b_2)$  if  $a_1 > a_2$  or  $a_1 = a_2$  and  $b_1 < b_2$ . Next, define an ordering on tuples of the form  $[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]$  such that the order is lexicographic in terms of the ordered pairs  $(a_{i,1}, a_{i,2})$  from left to right. Finally, define an ordering on the same tuples for  $s \geq 0$  such that

$$[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r+s,1}, a_{r+s,2})] \succ [(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})].$$

For example,  $(3, 1) \succ (3, 2) \succ (2, 0)$  and  $[(6, 5), (4, 2)] \succ [(6, 5), (4, 3)] \succ [(5, 2), (2, 0)]$ .

**Lemma 2.3.** *Suppose*

$$N > a_{1,1} > a_{1,2} \geq a_{2,1} > a_{2,2} \geq \dots \geq a_{r,1} > a_{r,2} \geq 0 = a_{r+1,1} = a_{r+1,2} = \dots = a_{r+s,1} = a_{r+s,2}$$

*and after setting*

$$a_{0,1} = a_{0,2} = N, \quad a_{r+1,1} = a_{r+1,2} = 0, \quad j_{r+1} = k_{r+1} = 0,$$

*that (or else  $[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]$  is empty)*

$$a_{i-1,1} \geq 2a_{i,1} - a_{i,2} \quad \text{for } 1 \leq i \leq r.$$

*Let*

$$C = \{(j_1, \dots, j_r) : \max(a_{i+1,2}, 2a_{i,2} - a_{i,1}) \leq j_i \leq \max(a_{i,2} - 1, 0), 1 \leq i \leq r\},$$

$$D = \{(k_1, \dots, k_r) : a_{i,2} \leq k_i \leq a_{i,1} - 1, 1 \leq i \leq r\}.$$

*Then*

$$\begin{aligned} & |[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r+s,1}, a_{r+s,2})]| \\ &= |[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]| \\ &= \sum_{(j_1, \dots, j_r) \in C} |[(a_{1,2}, j_1), (a_{2,2}, j_2), \dots, (a_{r,2}, j_r)]| \prod_{i=1}^r \left[ \frac{a_{i-1,2} - (2a_{i,2} - j_i)}{a_{i,1} - (2a_{i,2} - j_i)} \right]_q \\ &\quad - \sum_{(k_1, \dots, k_r) \in D \setminus (a_{1,2}, \dots, a_{r,2})} |[(a_{1,1}, k_1), (a_{2,1}, k_2), \dots, (a_{r,1}, k_r)]| \prod_{i=1}^r \left[ \frac{k_i - a_{i+1,1}}{a_{i,2} - a_{i+1,1}} \right]_q. \end{aligned}$$

*Proof.* We give an example before the general case. Let  $r = 2$ ; we compute  $|[(3, 1), (1, 0)]|$  by counting  $|\langle [3, 1], [1, 0] \rangle|$  in two different ways. Applying Proposition 2.2 to the terms on the left within the brackets gives

$$|\langle [3, 1], [1, 0] \rangle| = |\langle [(3, 2), 1], [(1, 0), 0] \rangle| + |\langle [(3, 1), 1], [(1, 0), 0] \rangle|.$$

Above, if  $(W_1, W_2, W_3, W_4) \in \langle [(3, 2), 1], [(1, 0), 0] \rangle$  then  $W_2 = W_3$  and  $W_4 = \{0\}$ . So

$$| \langle [(3, 2), 1], [(1, 0), 0] \rangle | = | [(3, 2), (1, 0)] |.$$

Likewise for  $(W_1, W_2, W_3, W_4) \in \langle [(3, 1), 1], [(1, 0), 0] \rangle$  then  $W_2 = W_3$  and  $W_4 = \{0\}$ . So

$$| \langle [(3, 1), 1], [(1, 0), 0] \rangle | = | [(3, 1), (1, 0)] |,$$

and

$$| \langle [3, 1], [1, 0] \rangle | = | [(3, 2), (1, 0)] | + | [(3, 1), (1, 0)] |.$$

Next, applying Proposition 2.2 to the terms on the right within the brackets gives

$$| \langle [3, 1], [1, 0] \rangle | = | \langle [3, (1, 0)], [1, (0, 0)] \rangle |.$$

If  $(W_1, W_2, W_3, W_4) \in \langle [3, (1, 0)], [1, (0, 0)] \rangle$ , then  $W_3 = W_2$ ,  $W_4 = \{0\}$  and thus  $W_1$  is a 3-dimensional subspace containing the 2-dimensional space  $W_2 + \sigma W_2$ . So

$$| \langle [3, (1, 0)], [1, (0, 0)] \rangle | = | [(1, 0), (0, 0)] | \begin{bmatrix} N-2 \\ 1 \end{bmatrix}_q,$$

and therefore

$$| \langle [3, (1, 0)], [1, (0, 0)] \rangle | = | [(1, 0), (0, 0)] | \begin{bmatrix} N-2 \\ 1 \end{bmatrix}_q.$$

We then have, after rearranging, that

$$| [(3, 1), (1, 0)] | = | [(1, 0), (0, 0)] | \begin{bmatrix} N-2 \\ 1 \end{bmatrix}_q - | [(3, 2), (1, 0)] |.$$

Note that

$$[(3, 2), (1, 0)], [(1, 0), (0, 0)]$$

come before  $[(3, 1), (1, 0)]$  in the ordering on tuples.

The proof of the Lemma is a generalization of this process. The first equality is clear. The size of  $[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]$  is computed by applying Proposition 2.2

$$\begin{aligned} & | \langle [a_{1,1}, a_{1,2}], [a_{2,1}, a_{2,2}], \dots, [a_{r,1}, a_{r,2}] \rangle | \\ &= \sum_{(k_1, \dots, k_r) \in D} | \langle [(a_{1,1}, k_1), a_{1,2}], [(a_{2,1}, k_2), a_{2,2}], \dots, [(a_{r,1}, k_r), a_{r,2}] \rangle | \\ \text{(R)} \quad &= \sum_{(k_1, \dots, k_r) \in D} | [(a_{1,1}, k_1), (a_{2,1}, k_2), \dots, (a_{r,1}, k_r)] | \prod_{i=1}^r \begin{bmatrix} k_i - a_{i+1,1} \\ a_{i,2} - a_{i+1,1} \end{bmatrix}_q. \end{aligned}$$

Expanding in the other way, we get

$$\begin{aligned} & | \langle [a_{1,1}, a_{1,2}], [a_{2,1}, a_{2,2}], \dots, [a_{r,1}, a_{r,2}] \rangle | \\ &= \sum_{(j_1, \dots, j_r) \in C} | \langle [a_{1,1}, (a_{1,2}, j_1)], [a_{2,1}, (a_{2,2}, j_2)], \dots, [a_{r,1}, (a_{r,2}, j_r)] \rangle | \\ \text{(L)} \quad &= \sum_{(j_1, \dots, j_r) \in C} | [(a_{1,2}, j_1), (a_{2,2}, j_2), \dots, (a_{r,2}, j_r)] | \prod_{i=1}^r \begin{bmatrix} a_{i-1,2} - (2a_{i,2} - j_i) \\ a_{i,1} - (2a_{i,2} - j_i) \end{bmatrix}_q. \end{aligned}$$

Subtracting from (R) and (L) the quantity

$$|[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]|$$

produces the stated result of the Lemma.  $\square$

Finally, we relate sets of the form  $[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]$  to  $\sigma$ -splitting subspaces.

**Proposition 2.4.** *Let  $\mathbb{F}_{q^N} = \mathbb{F}_{q^{mn}}$ . Then*

$$\begin{aligned} & |[(n-1)m, (n-2)m), ((n-2)m, (n-3)m), \dots, (2m, m), (m, 0)]| \\ &= \left\{ \left( \bigoplus_{i=0}^{n-2} \sigma^i W, \bigoplus_{i=0}^{n-3} \sigma^i W, \dots, W \oplus \sigma W, W \right) : \bigoplus_{i=0}^{n-1} \sigma^i W = \mathbb{F}_{q^{mn}} \right\}. \end{aligned}$$

*In particular  $|[(n-1)m, (n-2)m), ((n-2)m, (n-3)m), \dots, (2m, m), (m, 0)]|$  is the number of  $\sigma$ -splitting subspaces.*

*Proof.* If  $W$  is a  $\sigma$ -splitting subspace, then

$$\begin{aligned} & \left( \bigoplus_{i=0}^{n-2} \sigma^i W, \bigoplus_{i=0}^{n-3} \sigma^i W, \dots, W \oplus \sigma W, W \right) \\ & \in [((n-1)m, (n-2)m), ((n-2)m, (n-3)m), \dots, (2m, m), (m, 0)]. \end{aligned}$$

On the other hand, suppose that

$$(W_{n-1}, \dots, W_1) \in [((n-1)m, (n-2)m), ((n-2)m, (n-3)m), \dots, (2m, m), (m, 0)]$$

Then for  $1 \leq k \leq n-2$

$$\begin{aligned} \dim(W_{k+1}) &= (k+1)m \\ &= 2km - (k-1)m \\ &= \dim(W_k + \sigma W_k). \end{aligned}$$

So  $W_{k+1} = W_k + \sigma W_k$  for  $1 \leq k \leq n-2$ . Also,  $W_2 = W_1 \oplus \sigma W_1$  as  $W_1 \cap \sigma W_1 = \{0\}$ .

Suppose that  $W_k = \bigoplus_{i=0}^{k-1} \sigma^i W_1$ . Then, since  $\dim(W_{k+1}) = \dim(W_k + \sigma W_k) = (k+1)m$ , we obtain

$$\begin{aligned} W_{k+1} &= W_k + \sigma W_k \\ &= W_1 + \sigma W_1 + \dots + \sigma^k W_1 \\ &= \bigoplus_{i=0}^k \sigma^i W_1. \end{aligned}$$

When  $k = n-1$ , we have that  $W_{n-1} + \sigma W_{n-1} = \bigoplus_{i=0}^{n-1} \sigma^i W_1$ , since  $W_{n-1} + \sigma W_{n-1} = \mathbb{F}_{q^{mn}}$  is  $mn$ -dimensional. So  $W_1$  is indeed a  $\sigma$ -splitting subspace.  $\square$

**Corollary 2.5.** *The number of  $\sigma$ -splitting subspaces in  $\mathbb{F}_{q^{mn}}$  over  $F_q$  is independent of choice of primitive element  $\sigma$ .*

*Proof.* Neither the base case  $|[(0, 0)]|$  nor Lemma 2.3 depends on the  $\sigma$  chosen.  $\square$

**Remark.** More generally, given an arbitrary invertible linear operator  $T$  on  $\mathbb{F}_{q^{mn}}$  over  $\mathbb{F}_q$ , we might consider how many “ $T$ -splitting” subspaces exist; that is, the number of  $m$ -dimensional subspaces  $W$  such that

$$W \oplus TW \oplus \cdots \oplus T^{n-1}W = \mathbb{F}_{q^{mn}}.$$

We may then redefine  $(\cdot, \cdot), [\cdot, \cdot], \langle \cdot, \cdot \rangle$  by replacing the expressions  $W + \sigma W$  with  $W + TW$  and  $W \cap \sigma^{-1}W$  with  $W \cap T^{-1}W$ .

Recall from Proposition 2.1 and Lemma 2.3 that when  $T(v) = \sigma v$ , the nonzero numbers  $|[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]|$  can be computed from the base case  $|[0, 0]| = 1$ . But if  $T$  is any invertible linear operator, there may exist nonempty sets of the form  $[(a_1, a_1), (a_2, a_2), \dots, (a_r, a_r)]$  where  $a_r \neq 0$ . In fact, such sets cannot be computed recursively. For example

$$\begin{aligned} & | \langle [4, 4], [2, 2] \rangle | \\ &= | \langle [(4, 4), 4], [(2, 2), 2] \rangle | = |[(4, 4), (2, 2)]| \\ &= | \langle [4, (4, 4)], [2, (2, 2)] \rangle | = |[(4, 4), (2, 2)]|. \end{aligned}$$

We may still apply Lemma 2.3 in the case of general  $T$ , however, with the cardinalities of these sets as additional base cases.

### 3. SOLUTION TO THE RECURSION

The next two lemmas are special cases of the following  $q$ -Chu-Vandermonde identity for  $N$  a nonnegative integer [1, p. 354].

$$\begin{aligned} {}_2\phi_1 \left( \begin{matrix} q^{-N}, & a; & cq^N/a \\ & c \end{matrix} \right) &:= \sum_{m=0}^N \frac{(q^{-N}; q)_m (a; q)_m}{(q; q)_m (c; q)_m} \left( \frac{cq^N}{a} \right)^m \\ &= \frac{(c/a; q)_N}{(c; q)_N}. \end{aligned}$$

**Lemma 3.1.** *If  $C \leq B - 1 \leq D - 1 \leq A - 1$  are non-negative integers, then*

$$\begin{aligned} & \sum_{s=C}^{B-1} \begin{bmatrix} A - B - 1 \\ B - s - 1 \end{bmatrix}_q \begin{bmatrix} B \\ s \end{bmatrix}_q \begin{bmatrix} s \\ C \end{bmatrix}_q \begin{bmatrix} A - (2B - s) \\ D - (2B - s) \end{bmatrix}_q q^{(B-s)(B-s-1)} \\ &= \frac{[B]_q}{[D - C]_q} \begin{bmatrix} B - 1 \\ C \end{bmatrix}_q \begin{bmatrix} A - B - 1 \\ D - B - 1 \end{bmatrix}_q \begin{bmatrix} D - C \\ B - C \end{bmatrix}_q. \end{aligned}$$

**Lemma 3.2.** *If  $C \leq D \leq B - 1 \leq A - 1$  are non-negative integers, then*

$$\begin{aligned} & \sum_{s=D}^{B-1} \begin{bmatrix} A - B - 1 \\ B - s - 1 \end{bmatrix}_q \begin{bmatrix} B \\ s \end{bmatrix}_q \begin{bmatrix} s \\ C \end{bmatrix}_q \begin{bmatrix} s - C \\ D - C \end{bmatrix}_q q^{(B-s)(B-s-1)} \\ &= \frac{[B]_q}{[A - D]_q} \begin{bmatrix} B - 1 \\ C \end{bmatrix}_q \begin{bmatrix} B - C - 1 \\ D - C \end{bmatrix}_q \begin{bmatrix} A - D \\ B - D \end{bmatrix}_q. \end{aligned}$$

We now give our main theorem.

**Theorem 3.3.** *Suppose that*

$$N > a_{1,1} > a_{1,2} \geq a_{2,1} > a_{2,2} \geq \cdots \geq a_{r,1} > a_{r,2} \geq 0, \\ a_{0,1} = a_{0,2} = N, \quad a_{r+1,1} = a_{r+1,2} = 0.$$

*Then*

$$(1) \quad |[(a_{1,1}, a_{1,2}), \dots, (a_{r,1}, a_{r,2})]| = \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} a_{1,1} \\ 1 \end{bmatrix}_q} \frac{\prod_{i=0}^{r-1} \begin{bmatrix} a_{i,1} - a_{i+1,1} - 1 \\ a_{i+1,1} - a_{i+1,2} - 1 \end{bmatrix}_q \begin{bmatrix} a_{i+1,1} \\ a_{i+1,2} \end{bmatrix}_q}{\prod_{i=1}^{r-1} \begin{bmatrix} a_{i,1} - 1 \\ a_{i+1,1} - 1 \end{bmatrix}_q} q^E,$$

*where*

$$E = \sum_{i=1}^r (a_{i,1} - a_{i,2})(a_{i,1} - a_{i,2} - 1).$$

**Corollary 3.4** (Splitting Subspace Conjecture). *We have, when  $N \geq mn$ , the equality*

$$|[(n-1)m, (n-2)m), \dots, (2m, m), (m, 0)]| = \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} m \\ 1 \end{bmatrix}_q} \begin{bmatrix} N - mn + m - 1 \\ m - 1 \end{bmatrix}_q q^{m(m-1)(n-1)}$$

*In particular, when  $N = mn$ ,*

$$|[(n-1)m, (n-2)m), \dots, (2m, m), (m, 0)]| = \frac{\begin{bmatrix} mn \\ 1 \end{bmatrix}_q}{\begin{bmatrix} m \\ 1 \end{bmatrix}_q} q^{m(m-1)(n-1)}.$$

*Proof.* From plugging into (1)

$$\begin{aligned} & |[(n-1)m, (n-2)m), ((n-2)m, (n-3)m), \dots, (2m, m), (m, 0)]| \\ &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} (n-1)m \\ 1 \end{bmatrix}_q} \frac{\left( \begin{bmatrix} N - (n-1)m - 1 \\ m-1 \end{bmatrix}_q \begin{bmatrix} m-1 \\ m-1 \end{bmatrix}_q \cdots \begin{bmatrix} m-1 \\ m-1 \end{bmatrix}_q \right) \left( \begin{bmatrix} (n-1)m \\ (n-2)m \end{bmatrix}_q \cdots \begin{bmatrix} m \\ 0 \end{bmatrix}_q \right)}{\begin{bmatrix} (n-1)m-1 \\ (n-2)m-1 \end{bmatrix}_q \cdots \begin{bmatrix} m-1 \\ 0 \end{bmatrix}_q} q^{\sum_{i=1}^{n-1} m(m-1)} \\ &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} (n-1)m \\ 1 \end{bmatrix}_q} \begin{bmatrix} N - (n-1)m - 1 \\ m-1 \end{bmatrix}_q \frac{\begin{bmatrix} (n-1)m \\ (n-2)m \end{bmatrix}_q \cdots \begin{bmatrix} 2m \\ m \end{bmatrix}_q}{\begin{bmatrix} (n-1)m-1 \\ (n-2)m-1 \end{bmatrix}_q \cdots \begin{bmatrix} m-1 \\ 0 \end{bmatrix}_q} q^{m(m-1)(n-1)}. \\ &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} (n-1)m \\ 1 \end{bmatrix}_q} \begin{bmatrix} N - (n-1)m - 1 \\ m-1 \end{bmatrix}_q \frac{1 - q^{(n-1)m}}{1 - q^m} q^{m(m-1)(n-1)} \\ &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} m \\ 1 \end{bmatrix}_q} \begin{bmatrix} N - mn + m - 1 \\ m-1 \end{bmatrix}_q q^{m(m-1)(n-1)}. \end{aligned}$$

□

*Proof of Theorem 3.3.* We verify that (1) satisfies the recursion in Lemma 2.3.

Recall that

$$L = \sum_{(j_1, \dots, j_r) \in C} |[(a_{1,2}, j_1), (a_{2,2}, j_2), \dots, (a_{r,2}, j_r)]| \prod_{i=1}^r \begin{bmatrix} a_{i-1,2} - (2a_{i,2} - j_i) \\ a_{i,1} - (2a_{i,2} - j_i) \end{bmatrix}_q, \\ R = \sum_{(k_1, \dots, k_r) \in D} |[(a_{1,1}, k_1), (a_{2,1}, k_2), \dots, (a_{r,1}, k_r)]| \prod_{i=1}^r \begin{bmatrix} k_i - a_{i+1,1} \\ a_{i,2} - a_{i+1,1} \end{bmatrix}_q.$$

We first check equality when  $a_{r,2} \neq 0$  so that the expressions obtained for (L) and (R) using (1) do not contain negative  $q$ -binomials.

Substituting (1) and applying Lemma 3.1 to the resulting independent sums in (L) gives

$$\begin{aligned} L &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q \prod_{i=1}^r \sum_{j_i} \begin{bmatrix} a_{i-1,2}-a_{i,2}-1 \\ a_{i,2}-j_i-1 \end{bmatrix}_q \begin{bmatrix} a_{i,2} \\ j_i \end{bmatrix}_q \begin{bmatrix} j_i \\ a_{i+1,2} \end{bmatrix}_q \begin{bmatrix} a_{i-1,2}-(2a_{i,2}-j_i) \\ a_{i,1}-(2a_{i,2}-j_i) \end{bmatrix}_q q^{(a_{i,2}-j_i)(a_{i,2}-j_i-1)}}{\prod_{i=1}^{r-1} \begin{bmatrix} a_{i,2}-1 \\ a_{i+1,2}-1 \end{bmatrix}_q} \\ &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} a_{1,2} \\ 1 \end{bmatrix}_q} \prod_{i=1}^r \frac{[a_{i,2}]_q}{[a_{i,1}-a_{i+1,2}]_q} \begin{bmatrix} a_{i,2}-1 \\ a_{i+1,2} \end{bmatrix}_q \begin{bmatrix} a_{i-1,2}-a_{i,2}-1 \\ a_{i,1}-a_{i,2}-1 \end{bmatrix}_q \begin{bmatrix} a_{i,1}-a_{i+1,2} \\ a_{i,2}-a_{i+1,2} \end{bmatrix}_q \prod_{i=1}^{r-1} \begin{bmatrix} a_{i,2}-1 \\ a_{i+1,2}-1 \end{bmatrix}_q^{-1}. \end{aligned}$$

Substituting (1) and applying Lemma 3.2 to the resulting independent sums in (R) gives

$$\begin{aligned} R &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q \prod_{i=1}^r \sum_{k_i} \begin{bmatrix} a_{i-1,1}-a_{i,1}-1 \\ a_{i,1}-k_i-1 \end{bmatrix}_q \begin{bmatrix} a_{i,1} \\ k_i \end{bmatrix}_q \begin{bmatrix} k_i \\ a_{i+1,1} \end{bmatrix}_q \begin{bmatrix} k_i-a_{i+1,1} \\ a_{i,2}-a_{i+1,1} \end{bmatrix}_q q^{(a_{i,1}-k_i)(a_{i,1}-k_i-1)}}{\prod_{i=1}^{r-1} \begin{bmatrix} a_{i,2}-1 \\ a_{i+1,2}-1 \end{bmatrix}_q} \\ &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} a_{1,1} \\ 1 \end{bmatrix}_q} \prod_{i=1}^r \frac{[a_{i,1}]_q}{[a_{i-1,1}-a_{i,2}]_q} \begin{bmatrix} a_{i,1}-1 \\ a_{i+1,1} \end{bmatrix}_q \begin{bmatrix} a_{i,1}-a_{i+1,1}-1 \\ a_{i,2}-a_{i+1,1} \end{bmatrix}_q \begin{bmatrix} a_{i-1,1}-a_{i,2} \\ a_{i,1}-a_{i,2} \end{bmatrix}_q \prod_{i=1}^{r-1} \begin{bmatrix} a_{i,1}-1 \\ a_{i+1,1}-1 \end{bmatrix}_q^{-1}. \end{aligned}$$

After simplification (see Appendix A)

$$(2) \quad L = R = \frac{[N]_q [N - a_{1,2} - 1]!_q}{[N - a_{1,1}]!_q [a_{r,2}]!_q} \prod_{i=1}^r \frac{[a_{i,1} - a_{i+1,2} - 1]!_q}{[a_{i,1} - a_{i,2} - 1]!_q [a_{i,1} - a_{i,2}]!_q} \prod_{i=2}^r \frac{1}{[a_{i-1,2} - a_{i,1}]!_q}.$$

Finally, we deal with the case  $a_{r,2} = 0$ , when the expression obtained by directly applying (1) to (L) may contain negative  $q$ -binomials ((R) is unaffected). Suppose  $r > 1$ . By definition, we know that

$$|\langle [a_{1,1}, a_{1,2}], [a_{2,1}, a_{2,2}], \dots, [a_{r,1}, 0] \rangle| = |\langle [a_{1,1}, a_{1,2}], [a_{2,1}, a_{2,2}], \dots, [a_{r-1,1}, a_{r-1,2}] \rangle| \begin{bmatrix} a_{r-1,2} \\ a_{r,1} \end{bmatrix}_q.$$

This means that

$$\begin{aligned} L &= \sum_{(j_1, \dots, j_r) \in C} |[(a_{1,2}, j_1), (a_{2,2}, j_2), \dots, (a_{r,2}, j_r)]| \prod_{i=1}^r \begin{bmatrix} a_{i-1,2} - (2a_{i,2} - j_i) \\ a_{i,1} - (2a_{i,2} - j_i) \end{bmatrix}_q \\ &= |\langle [a_{1,1}, a_{1,2}], \dots, [a_{r-1,1}, a_{r-1,2}] \rangle| \begin{bmatrix} a_{r-1,2} \\ a_{r,1} \end{bmatrix}_q. \end{aligned}$$

Since  $a_{r-1,2} \geq a_{r,1} > 0$ , we may apply our previous result to obtain

$$\begin{aligned} &|\langle [a_{1,1}, a_{1,2}], \dots, [a_{r-1,1}, a_{r-1,2}] \rangle| \begin{bmatrix} a_{r-1,2} \\ a_{r,1} \end{bmatrix}_q \\ &= \begin{bmatrix} a_{r-1,2} \\ a_{r,1} \end{bmatrix}_q \frac{[N]_q [N - a_{1,2} - 1]!_q}{[N - a_{1,1}]!_q [a_{r,2}]!_q} \prod_{i=1}^{r-1} \frac{[a_{i,1} - a_{i+1,2} - 1]!_q}{[a_{i,1} - a_{i,2} - 1]!_q [a_{i,1} - a_{i,2}]!_q} \prod_{i=2}^{r-1} \frac{1}{[a_{i-1,2} - a_{i,1}]!_q}. \end{aligned}$$

We wish to show that this is equal to

$$\frac{[N]_q [N - a_{1,2} - 1]!_q}{[N - a_{1,1}]!_q [a_{r,2}]!_q} \prod_{i=1}^r \frac{[a_{i,1} - a_{i+1,2} - 1]!_q}{[a_{i,1} - a_{i,2} - 1]!_q [a_{i,1} - a_{i,2}]!_q} \prod_{i=2}^r \frac{1}{[a_{i-1,2} - a_{i,1}]!_q}$$



when  $a_{r,2} = 0$ . Take the quotient to find

$$\begin{aligned} & \frac{\frac{[N]_q [N - a_{1,2} - 1]!_q}{[N - a_{1,1}]!_q [a_{r,2}]!_q} \prod_{i=1}^r \frac{[a_{i,1} - a_{i+1,2} - 1]!_q}{[a_{i,1} - a_{i,2} - 1]!_q [a_{i,1} - a_{i,2}]!_q} \prod_{i=2}^r \frac{1}{[a_{i-1,2} - a_{i,1}]!_q}}{\left[ \begin{smallmatrix} a_{r-1,2} \\ a_{r,1} \end{smallmatrix} \right]_q \frac{[N]_q [N - a_{1,2} - 1]!_q}{[N - a_{1,1}]!_q [a_{r-1,2}]!_q} \prod_{i=1}^{r-1} \frac{[a_{i,1} - a_{i+1,2} - 1]!_q}{[a_{i,1} - a_{i,2} - 1]!_q [a_{i,1} - a_{i,2}]!_q} \prod_{i=2}^{r-1} \frac{1}{[a_{i-1,2} - a_{i,1}]!_q}} \\ &= \frac{[a_{r-1,2}]!_q \frac{[a_{r,1} - 1]!_q}{[a_{r,1} - 1]!_q [a_{r,1}]!_q} \frac{1}{[a_{r-1,2} - a_{r,1}]!_q}}{\left[ \begin{smallmatrix} a_{r-1,2} \\ a_{r,1} \end{smallmatrix} \right]_q} \\ &= 1, \end{aligned}$$

as desired. Therefore, when  $a_{r,2} = 0$ , the equality

$$\begin{aligned} L &= \sum_{(j_1, \dots, j_r) \in C} |[a_{1,2}, j_1), [a_{2,2}, j_2), \dots, [a_{r,2}, j_r)]| \prod_{i=1}^r \left[ \begin{smallmatrix} a_{i-1,2} - (2a_{i,2} - j_i) \\ a_{i,1} - (2a_{i,2} - j_i) \end{smallmatrix} \right]_q \\ &= \frac{[N]_q [N - a_{1,2} - 1]!_q}{[N - a_{1,1}]!_q [a_{r,2}]!_q} \prod_{i=1}^r \frac{[a_{i,1} - a_{i+1,2} - 1]!_q}{[a_{i,1} - a_{i,2} - 1]!_q [a_{i,1} - a_{i,2}]!_q} \prod_{i=2}^r \frac{1}{[a_{i-1,2} - a_{i,1}]!_q} \\ &= R \end{aligned}$$

still holds.

Finally, suppose  $r = 1$ . Then,

$$L = |[ (0, 0) ]| \left[ \begin{smallmatrix} N \\ a_{1,1} \end{smallmatrix} \right]_q = \left[ \begin{smallmatrix} N \\ a_{1,1} \end{smallmatrix} \right]_q.$$

If we plug in  $\langle [a_{1,1}, 0] \rangle$  into (2), then we get  $\left[ \begin{smallmatrix} N \\ a_{1,1} \end{smallmatrix} \right]_q$ , as desired.  $\square$

**Corollary 3.5.** *The numbers*

$$| \langle [a_{1,1}, a_{1,2}], [a_{2,1}, a_{2,2}], \dots, [a_{r,1}, a_{r,2}] \rangle |$$

are given by

$$L = R = \frac{[N]_q [N - a_{1,2} - 1]!_q}{[N - a_{1,1}]!_q [a_{r,2}]!_q} \prod_{i=1}^r \frac{[a_{i,1} - a_{i+1,2} - 1]!_q}{[a_{i,1} - a_{i,2} - 1]!_q [a_{i,1} - a_{i,2}]!_q} \prod_{i=2}^r \frac{1}{[a_{i-1,2} - a_{i,1}]!_q}.$$

#### 4. SPECIAL CASE: (K, K-1)

Note that when  $r = 1$  and  $a_{1,1} = k, a_{1,2} = k - 1$ , with  $k \leq N - 1$ , the formula (1) gives

$$|(k, k - 1)| = \left[ \begin{smallmatrix} N \\ 1 \end{smallmatrix} \right]_q,$$

a number independent of  $k$ .

**Proposition 4.1.** *There is a bijection between sets of the form  $(k_1, k_1 - 1)$  and  $(k_2, k_2 - 1)$  when  $k_1, k_2 \leq N - 1$ .*

*Proof.* It suffices to show that there exists a bijection between  $(k, k - 1)$  and  $(k - 1, k - 2)$  for  $2 \leq k \leq N - 1$ . Define

$$\begin{aligned} \phi : (k - 1, k - 2) &\rightarrow (k, k - 1) \\ W &\mapsto W + \sigma W. \end{aligned}$$

The map  $\phi$  is well defined:

$$\begin{aligned}\dim(W + \sigma W) &= k, \\ \dim((W + \sigma W) \cap (\sigma^{-1}W + W)) &= k - 1.\end{aligned}$$

The second equality follows from the fact that  $(W + \sigma W) \cap (\sigma^{-1}W + W)$  contains  $W$  and has dimension *strictly* less than  $k$  by Proposition 2.1.

Next,  $\phi$  is injective: if  $W_1, W_2 \in (k-1, k-2)$  and  $W_1 + \sigma W_1 = W_2 + \sigma W_2 = W' \in (k, k-1)$ , then  $W' \cap \sigma^{-1}W' = W_1 = W_2$ .

Finally,  $\phi$  is surjective: if  $W' \in (k, k-1)$ , then  $W' \cap \sigma^{-1}W' \in (k-1, k-2)$  since  $(W' \cap \sigma^{-1}W') + \sigma(W' \cap \sigma^{-1}W') \subseteq W'$ ; in fact  $(W' \cap \sigma^{-1}W') + \sigma(W' \cap \sigma^{-1}W') = W'$ .  $\square$

## 5. A $q = 1$ ANALOGUE

We might ask what (1) counts when  $q = 1$ ; indeed the situation translates from enumerating subspaces of vector spaces to enumerating subsets of sets.

Instead of subspaces of  $\mathbb{F}_{q^N}$ , we consider subsets of  $\{1, \dots, N\}$ . Rather than multiplying by the element  $\sigma$ , we let  $\sigma = (12 \cdots N)$  cyclically permute the elements of  $\{1, \dots, N\}$  so that  $\sigma$  preserves no proper subset, in analogy with Proposition 2.1; in fact, any permutation of  $\{1, \dots, N\}$  preserving no proper subset is cyclic. When  $N = mn$ , the number of  $m$ -element subsets  $W$  of  $\{1, \dots, N\}$  such that  $\bigcup_{i=0}^{n-1} \sigma^i W = \{1, \dots, N\}$  is clearly  $n$ ; this is true in a more general setting. We retain the  $[\ , \ ], ( \ , \ ), < \ , >$  notation with the definitions restated in the context of subsets of  $\{1, \dots, N\}$  below.

**Definition.** Suppose  $A_1, A_2, \dots, A_k$  are sets of subsets of  $\{1, \dots, N\}$ . Let  $[A_1, A_2, \dots, A_k]$  be the set of all  $k$ -tuples  $(W_1, W_2, \dots, W_k)$  such that

$$\begin{aligned}W_i &\in A_i \quad \text{for } 1 \leq i \leq k, \\ W_i &\supseteq W_{i+1} \cup \sigma W_{i+1} \quad \text{for } 1 \leq i \leq k-1.\end{aligned}$$

If  $A_i$  is the set of all subsets of  $\{1, \dots, N\}$  with cardinality  $d_i$ , then  $A_i$  is denoted within the brackets as  $d_i$ .

**Definition.** For nonnegative integers  $a, b$  with  $N > a > b$  or  $a = b = 0$

$$(a, b) := \{W \subseteq \{1, \dots, N\} : |W| = a, |W \cap \sigma^{-1}W| = b\}.$$

**Definition.** Given sets  $[A_{1,1}, A_{1,2}], [A_{2,1}, A_{2,2}], \dots, [A_{r,1}, A_{r,2}]$  as defined above, let

$$\langle [A_{1,1}, A_{1,2}], [A_{2,1}, A_{2,2}], \dots, [A_{r,1}, A_{r,2}] \rangle$$

denote the set of  $2r$ -tuples of subsets  $(W_{1,1}, W_{1,2}, W_{2,1}, W_{2,2}, \dots, W_{r,1}, W_{r,2})$  such that

$$\begin{aligned}(W_{i,1}, W_{i,2}) &\in [A_{i,1}, A_{i,2}] \quad \text{for } 1 \leq i \leq r, \\ W_{i,2} &\supseteq W_{i+1,1} \quad \text{for } 1 \leq i \leq r-1.\end{aligned}$$

Lemma 2.3 and our formulas in Theorem 3.3 and Corollaries 3.4 and 3.5 are still valid here by setting  $q = 1$ ; the  $q$ -binomials counting ways to extend subspaces become binomial terms counting ways to enlarge subsets. However, we can directly count some special cases.

An appropriate adaptation of Proposition 2.4 gives

$$[((n-1)m, (n-2)m), ((n-2)m, (n-3)m), \dots, (2m, m), (m, 0)]$$

$$= \left\{ \left( \bigcup_{i=0}^{n-2} \sigma^i W, \bigcup_{i=0}^{n-3} \sigma^i W, \dots, W \cup \sigma W, W \right) : \left| \bigcup_{i=0}^{n-1} \sigma^i W \right| = mn \text{ and } |W| = m \right\}.$$

Counting the number of ordered pairs  $(W, k)$  where  $W$  satisfies the conditions in the set above and  $k$  is an element of  $W$  in two different ways, one by fixing  $k$  first and the other by fixing  $W$  first, yields  $|\{((n-1)m, (n-2)m), \dots, (m, 0)\}| = \frac{N}{m} \binom{N-mn+m-1}{m-1}$ , which is the same as the formula from Corollary 3.4 when we set  $q = 1$ .

We may also count the elements of  $(m, k)$  directly by counting the number of ordered pairs  $(W, a)$  where  $W \in (m, k)$  and  $a \notin W$  in two ways, one by fixing  $W$  first and the other by fixing  $a$  first. This yields  $\frac{N}{N-m} \binom{N-m}{m-k} \binom{m-1}{k} = \frac{N}{m} \binom{N-m-1}{m-k-1} \binom{m}{k}$ . For  $q$  a power of a prime, (1) yields

$$|(m, k)| = \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} m \\ 1 \end{bmatrix}_q} \begin{bmatrix} N-m-1 \\ m-k-1 \end{bmatrix}_q \begin{bmatrix} m \\ k \end{bmatrix}_q q^{(m-k)(m-k-1)}.$$

This gives the same expression when  $q \rightarrow 1$  as obtained above.

## APPENDIX A. PROOF OF THEOREM 3.3, L=R

*Proof.*

$$\begin{aligned} L &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} a_{1,2} \\ 1 \end{bmatrix}_q} \prod_{i=1}^r \frac{[a_{i,2}]_q}{[a_{i,1} - a_{i+1,2}]_q} \begin{bmatrix} a_{i,2} - 1 \\ a_{i+1,2} \end{bmatrix}_q \begin{bmatrix} a_{i-1,2} - a_{i,2} - 1 \\ a_{i,1} - a_{i,2} - 1 \end{bmatrix}_q \begin{bmatrix} a_{i,1} - a_{i+1,2} \\ a_{i,2} - a_{i+1,2} \end{bmatrix}_q \prod_{i=1}^{r-1} \begin{bmatrix} a_{i,2} - 1 \\ a_{i+1,2} - 1 \end{bmatrix}_q^{-1} \\ &= \frac{\frac{[N]_q!}{[N-1]_q!}}{\frac{[a_{1,2}]_q!}{[a_{1,2}-1]_q!}} \frac{[a_{r,1} - 1]_q!}{[a_{r,2} - 1]_q!} \begin{bmatrix} a_{r-1,2} - a_{r,2} - 1 \\ a_{r,1} - a_{r,2} - 1 \end{bmatrix}_q \frac{1}{[a_{r,1} - a_{r,2}]_q!} \\ &\quad \prod_{i=1}^{r-1} \frac{[a_{i,2}]_q!}{[a_{i,2} - 1]_q!} \frac{[a_{i,1} - a_{i+1,2} - 1]_q!}{[a_{i+1,2}]_q!} \frac{[a_{i-1,2} - a_{i,2} - 1]_q!}{[a_{i,1} - a_{i,2} - 1]_q!} \frac{[a_{i+1,2} - 1]_q!}{[a_{i,1} - a_{i,2}]_q!} \\ &= \frac{\frac{[N]_q!}{[N-1]_q!}}{\frac{[a_{1,2}]_q!}{[a_{1,2}-1]_q!}} \frac{[a_{r,1} - 1]_q!}{[a_{r,2} - 1]_q!} \frac{[a_{r-1,2} - a_{r,2} - 1]_q!}{[a_{r,1} - a_{r,2} - 1]_q!} \frac{1}{[a_{r,1} - a_{r,2}]_q!} \\ &\quad \frac{[a_{1,2}]_q!}{[a_{r,2}]_q!} \frac{[a_{r,2} - 1]_q!}{[a_{1,2} - 1]_q!} \frac{[N - a_{1,2} - 1]_q!}{[a_{r-1,2} - a_{r,2} - 1]_q!} \prod_{i=1}^{r-1} \frac{[a_{i,1} - a_{i+1,2} - 1]_q!}{[a_{i,1} - a_{i,2} - 1]_q!} \frac{[a_{i-1,2} - a_{i,1}]_q!}{[a_{i,1} - a_{i,2}]_q!} \\ &= \frac{[N]_q!}{[N - a_{1,1}]_q!} \frac{[N - a_{1,2} - 1]_q!}{[a_{r,2}]_q!} \prod_{i=1}^r \frac{[a_{i,1} - a_{i+1,2} - 1]_q!}{[a_{i,1} - a_{i,2} - 1]_q!} \prod_{i=2}^r \frac{1}{[a_{i-1,2} - a_{i,1}]_q!}. \\ R &= \frac{\begin{bmatrix} N \\ 1 \end{bmatrix}_q}{\begin{bmatrix} a_{1,1} \\ 1 \end{bmatrix}_q} \prod_{i=1}^r \frac{[a_{i,1}]_q}{[a_{i-1,1} - a_{i,2}]_q} \begin{bmatrix} a_{i,1} - 1 \\ a_{i+1,1} \end{bmatrix}_q \begin{bmatrix} a_{i,1} - a_{i+1,1} - 1 \\ a_{i,2} - a_{i+1,1} \end{bmatrix}_q \begin{bmatrix} a_{i-1,1} - a_{i,2} \\ a_{i,1} - a_{i,2} \end{bmatrix}_q \prod_{i=1}^{r-1} \begin{bmatrix} a_{i,1} - 1 \\ a_{i+1,1} - 1 \end{bmatrix}_q^{-1} \\ &= \frac{\frac{[N]_q!}{[N-1]_q!}}{\frac{[a_{1,1}]_q!}{[a_{1,1}-1]_q!}} \frac{[a_{r,1}]_q!}{[a_{r,2}]_q!} \frac{[a_{r-1,1} - a_{r,2} - 1]_q!}{[a_{r,1} - a_{r,2} - 1]_q!} \frac{1}{[a_{r,1} - a_{r,2}]_q!} \frac{1}{[a_{r-1,1} - a_{r,1}]_q!} \end{aligned}$$

$$\begin{aligned}
& \prod_{i=1}^{r-1} \frac{[a_{i,1}]!_q}{[a_{i-1,1} - a_{i,2}]!_q} \frac{[a_{i-1,1} - a_{i,2} - 1]!_q}{[a_{i+1,1}]!_q} \frac{1}{[a_{i,2} - a_{i+1,1}]!_q [a_{i,1} - a_{i,2} - 1]!_q} \frac{[a_{i-1,1} - a_{i,2}]!_q}{[a_{i,1} - a_{i,2}]!_q [a_{i-1,1} - a_{i,1}]!_q} \\
&= \frac{\frac{[N]!_q}{[N-1]!_q}}{\frac{[a_{1,1}]!_q}{[a_{1,1}-1]!_q}} \frac{[a_{r,1}]!_q [a_{r-1,1} - a_{r,2} - 1]!_q}{[a_{r,2}]!_q [a_{r,1} - a_{r,2} - 1]!_q [a_{r,1} - a_{r,2}]!_q [a_{r-1,1} - a_{r,1}]!_q} \\
&= \frac{[a_{1,1}]!_q [a_{r,1} - 1]!_q [a_{r-1,1} - a_{r,1}]!_q}{[a_{r,1}]!_q [a_{1,1} - 1]!_q [N - a_{1,1}]!_q} \prod_{i=1}^{r-1} \frac{[a_{i-1,1} - a_{i,2} - 1]!_q}{[a_{i,2} - a_{i+1,1}]!_q [a_{i,1} - a_{i,2} - 1]!_q [a_{i,1} - a_{i,2}]!_q} \\
&= \frac{[N]_q [N - a_{1,2} - 1]!_q}{[N - a_{1,1}]!_q [a_{r,2}]!_q} \prod_{i=1}^r \frac{[a_{i,1} - a_{i+1,2} - 1]!_q}{[a_{i,1} - a_{i,2} - 1]!_q [a_{i,1} - a_{i,2}]!_q} \prod_{i=2}^r \frac{1}{[a_{i-1,2} - a_{i,1}]!_q}.
\end{aligned}$$

□

## ACKNOWLEDGEMENTS

This research was conducted at the 2012 summer REU (Research Experience for Undergraduates) program at the University of Minnesota, Twin Cities, and was supported by NSF grants DMS-1001933 and DMS-1148634. We would like to thank Gregg Musiker, Pavlo Pylyavskyy, Vic Reiner, and Dennis Stanton, who directed the program, for their support, and express particular gratitude to Dennis Stanton both for introducing us to this problem and for his indispensable guidance throughout the research process. We would further like to thank Alex Miller for his assistance in editing this report as well as Sudhir Ghorpade and Samrith Ram for their helpful comments.

## REFERENCES

- [1] G. Gasper and M. Rahman, *Basic Hypergeometric Series*, Enc. of Math. and its Appl., Vol. 96, Cambridge University Press, Cambridge, 2004.
- [2] S. R. Ghorpade, S. U. Hasan and M. Kumari, Primitive polynomials, Singer cycles, and word-oriented linear feedback shift registers, *Des. Codes Cryptogr.* **58** (2011), 123-134.
- [3] S. R. Ghorpade and S. Ram, Enumeration of splitting subspaces over finite fields, Arithmetic, Geometry, and Coding Theory, (Luminy, France, March 2011), Y. Aubry, C. Ritzenthaler and A. Zykin Eds., *Contemporary Mathematics*, Vol. 574, American Mathematical Society, Providence, RI, 2012, pp. 49-58.
- [4] H. Niederreiter, The multiple-recursive matrix method for pseudorandom number generation, *Finite Fields Appl.* **1** (1995), 3-30.
- [5] G. Zeng, W. Han and K. He, High efficiency feedback shift register:  $\sigma$ -LFSR, *Cryptology e-Print Archive: Report 2007/114* (available: <http://eprint.iacr.org/2007/114>).

ERIC CHEN, PRINCETON UNIVERSITY, PRINCETON, NJ 08544  
*E-mail address:* [ecchen@princeton.edu](mailto:ecchen@princeton.edu)

DENNIS TSENG, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139  
*E-mail address:* [DennisCTseng@gmail.com](mailto:DennisCTseng@gmail.com)